Engineering Safety- and Security-Related Requirements for Software-Intensive Systems

Presented at SSTC 2010

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Donald Firesmith, Terry Roberts &
Stephen Blanchette, Jr.

27 April 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 APR 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Engineering Safety- and Security-Related Requirements for Software-Intensive Systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 22nd Systems and Software Technology Conference (SSTC), 26-29 April 2010, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**48**	

Contents

Three Disciplines:

Requirements, Safety, and Security Engineering

Three Related Disciplines

Safety Engineering

> the engineering discipline within systems engineering concerned with lowering the risk of *unintentional unauthorized* harm to valuable assets to a level that is acceptable to the system's stakeholders by preventing, detecting, and reacting to such harm, mishaps (i.e., accidents and incidents), hazards, vulnerabilities, and safety risks

Security Engineering

> the engineering discipline within systems engineering concerned with lowering the risk of *intentional unauthorized* harm to valuable assets to a level that is acceptable to the system's stakeholders by preventing, detecting, and reacting to such harm, misuses (i.e., attacks and incidents), threats, vulnerabilities, and security risks

Requirements Engineering

> the engineering discipline within systems/software engineering concerned with identifying, analyzing, reusing, specifying, managing, verifying, and validating goals and requirements (including safety- and security-related requirements)

Challenges:

Combining Requirements, Safety, and Security Engineering

Challenges$_1$

Requirements engineering, safety engineering, and security engineering have different:

- *Communities*
- *Disciplines* with different training, books, journals, and conferences
- *Professions* with different *job titles*
- Fundamental underlying *concepts* and *terminologies*
- *Tasks, techniques,* and *tools*

Safety and security engineering are:

- Typically treated as *secondary specialty engineering* disciplines
- Performed separately from, largely Independently of, and lagging behind the primary engineering workflow:
  (requirements, architecture, design, etc.)

Challenges$_2$

Current separate methods for performing requirements, safety, and security engineering are inefficient and ineffective.

Separation of requirements engineering, safety engineering, and security engineering:

- Causes *poor* safety- and security-related requirements that are often:
  - Vague/unverifiable/unfeasible architectural and design constraints
  - Capabilities or goals rather than requirements
  - Inadequate and too late to drive architecture development and test planning
- Makes it unnecessarily difficult to achieve certification and accreditation for safe/secure operations

Challenges$_3$

Poor requirements are a primary cause of more than half of all project failures (defined in terms of):

- Major Cost Overruns
- Major Schedule Overruns
- Major Functionality not delivered
- Cancelled Projects
- Delivered Systems that are never used

Poor requirements are a major root cause of many (or most) accidents involving software-intensive systems.

Security ‘requirements’ often mandated (e.g., Industry Best Practices, Security Functions)

- Often, these are not derived into meaningful requirements at the engineering level

Challenges$_4$

Constant tension: How safe and secure is safe and secure *enough*?

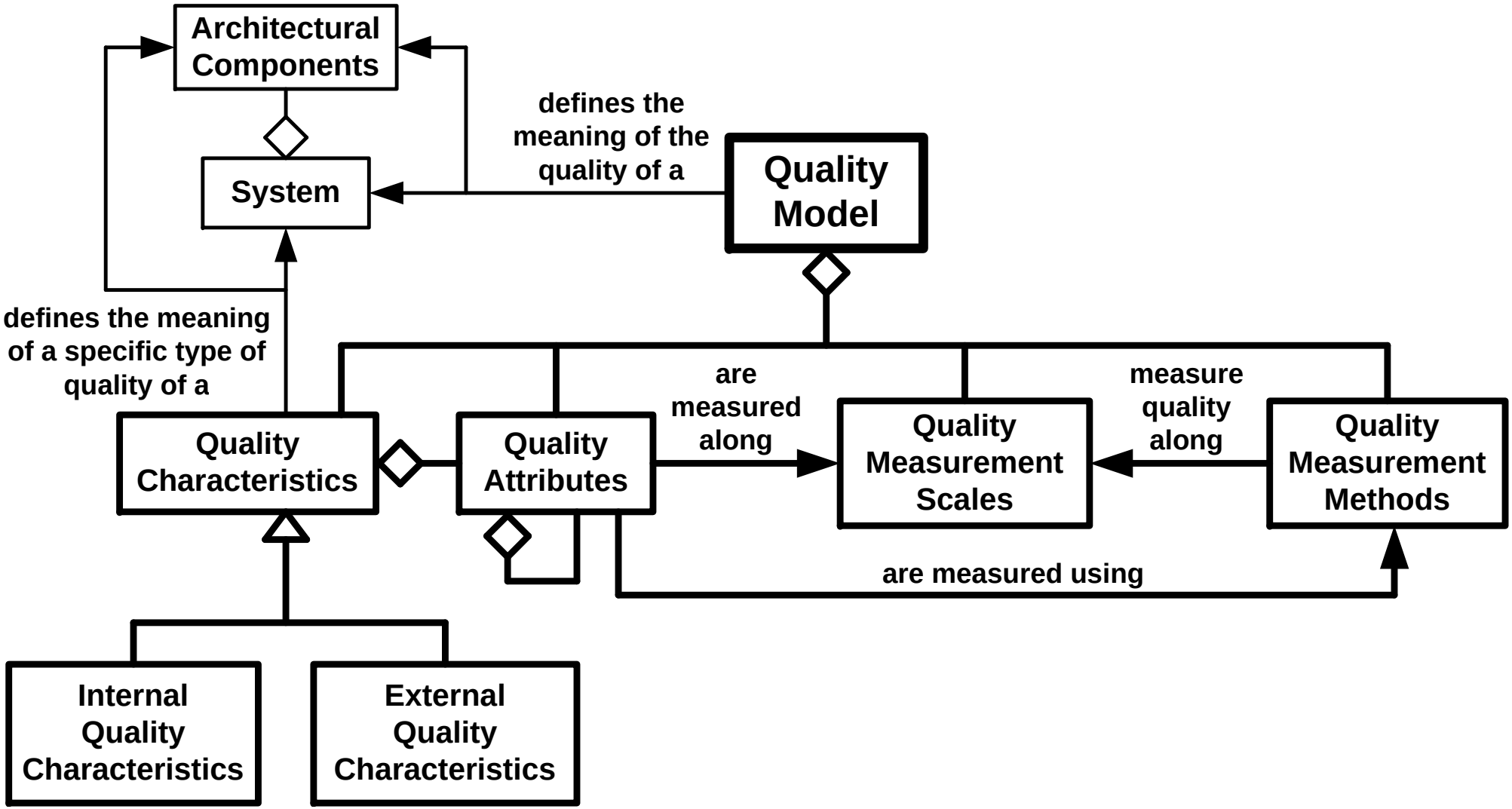
What is needed:

- Better consistency between safety and security engineering
  - More consistent concepts and terminology
  - Reuse of techniques across disciplines
  - Less unnecessary overlap and avoidance of redundant work
- Better collaboration:
  - Between safety and security engineering
  - With requirements engineering
- Better safety- and security-related requirements

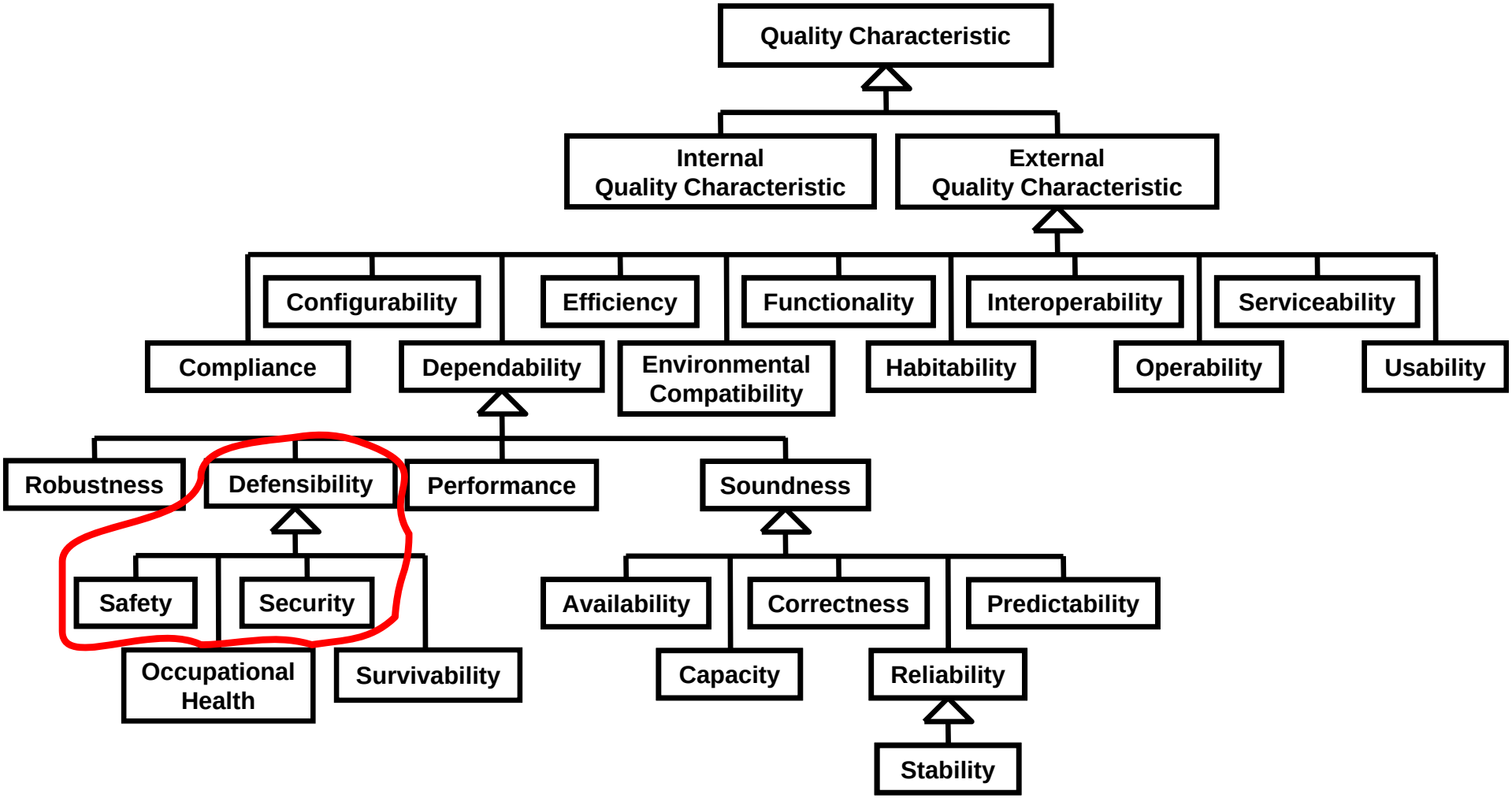
Fundamental Concepts:

A Foundation for Understanding

Quality Model



Quality Characteristics (External)



Defensibility$_1$

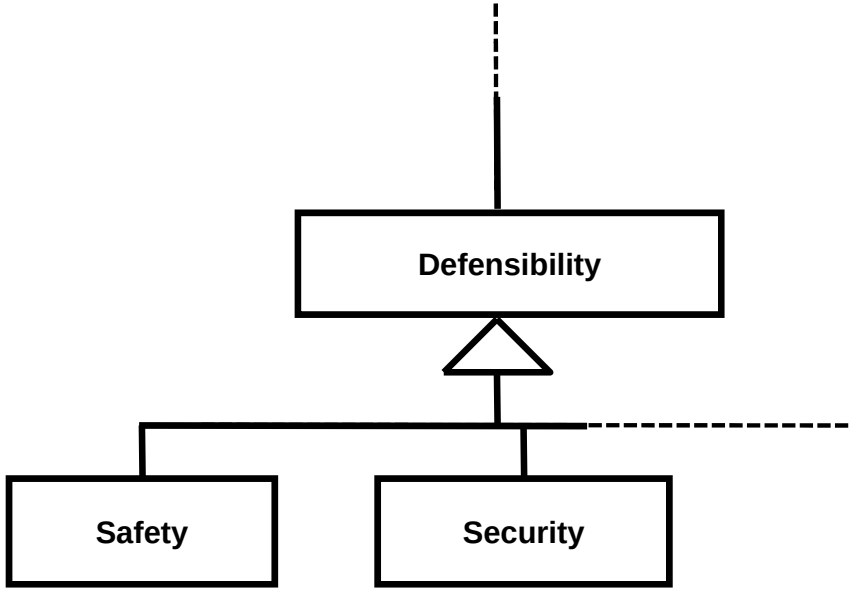
Defensibility

the quality characteristic capturing the degree to which the system:

- Properly prevents, detects, reacts to, and adapts to:
  - Unintended and unauthorized *harm* to *valuable assets* due to the occurrence of
  - *Abuses* enabled by the existence of
  - *Dangers*
- Has *defensibility risks* that are acceptably low to its *stakeholders*
- Valuable Assets may be people, organizations, property, services, or environments
- Harm may be direct or indirect, intentional or unintentional, authorized or unauthorized

Defensibility$_2$

Safety and security aspects of defensibility are defined in a similar manner by replacing:



- Abuse with either mishap (safety) or misuse (security)
- Danger with either hazard (safety) or threat (security)
- Defensibility risks with safety risks and security risks

Safety- and Security-Related Requirements

There's More Than One Type

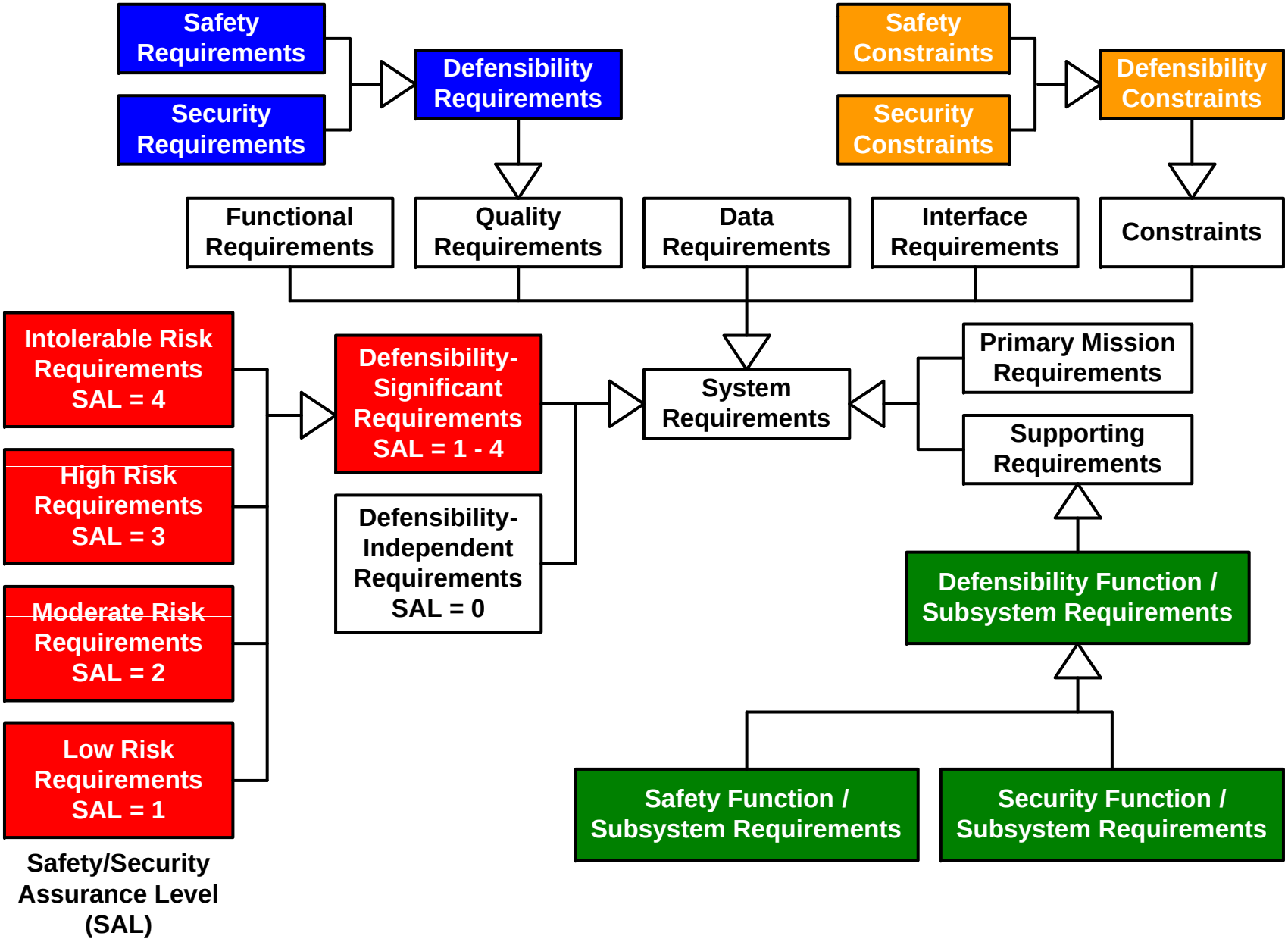
Too often, only a single type of requirements is considered when there are many types that need consideration:

- Special non-functional requirements:
  - Safety and security requirements *are* quality requirements
- Safety- and security-*significant* requirements (functional, data, and interface)
- Safety and security functions/subsystems requirements
- Safety and security *constraints*:
  - Architectural and design constraints
  - Mandated defensibility controls (i.e., safeguards and countermeasures)

Separation of safety/security/requirements engineering almost assures gaps in requirements

Gaps in Requirements Lead to Shortcomings in Delivered Systems

Four Types of Defensibility-Related Requirements



Example Safety- and Security-Related Requirements

Safety / Security Requirement

- "When in mode V, the system shall limit the occurrence of *accidental harm* of type W to valuable assets of type X to an average rate of no more than Y asset value per Z time duration."
- "When in mode X, the system shall *detect misuses* of type Y an average of at least Z percent of the time."

Safety / Security Significant Requirement

- "The system shall automatically transport passengers between stations."
- "The system shall enable users to update their personal information."

Safety / Security Function / Subsystem Requirement

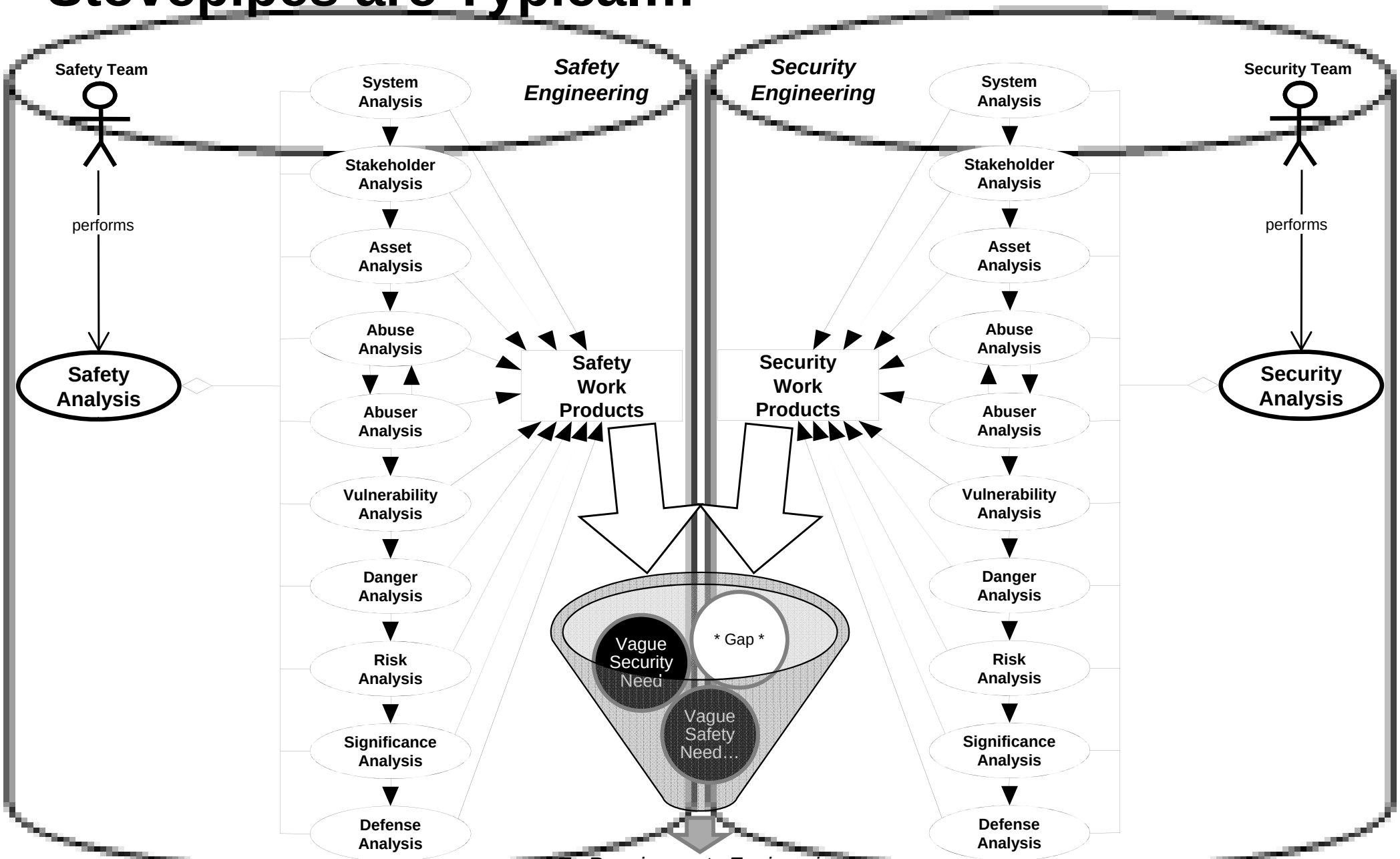
- "The system shall include a fire detection and suppression subsystem."
- "The system shall support the encryption/decryption of sensitive data."

Safety / Security Constraint

- "The system shall not contain any of the hazardous materials in Table X."
- "The system shall use passwords for user authentication."

Collaboratively Engineering Safety- & Security-Related Requirements

Stovepipes are Typical…



A Better Way

Ensure close collaboration among Safety, Security, and Requirements Teams

Better Integrate Safety and Security Methods:

- Concepts and Terminology
- Techniques and Work Products
- Provide Cross Training

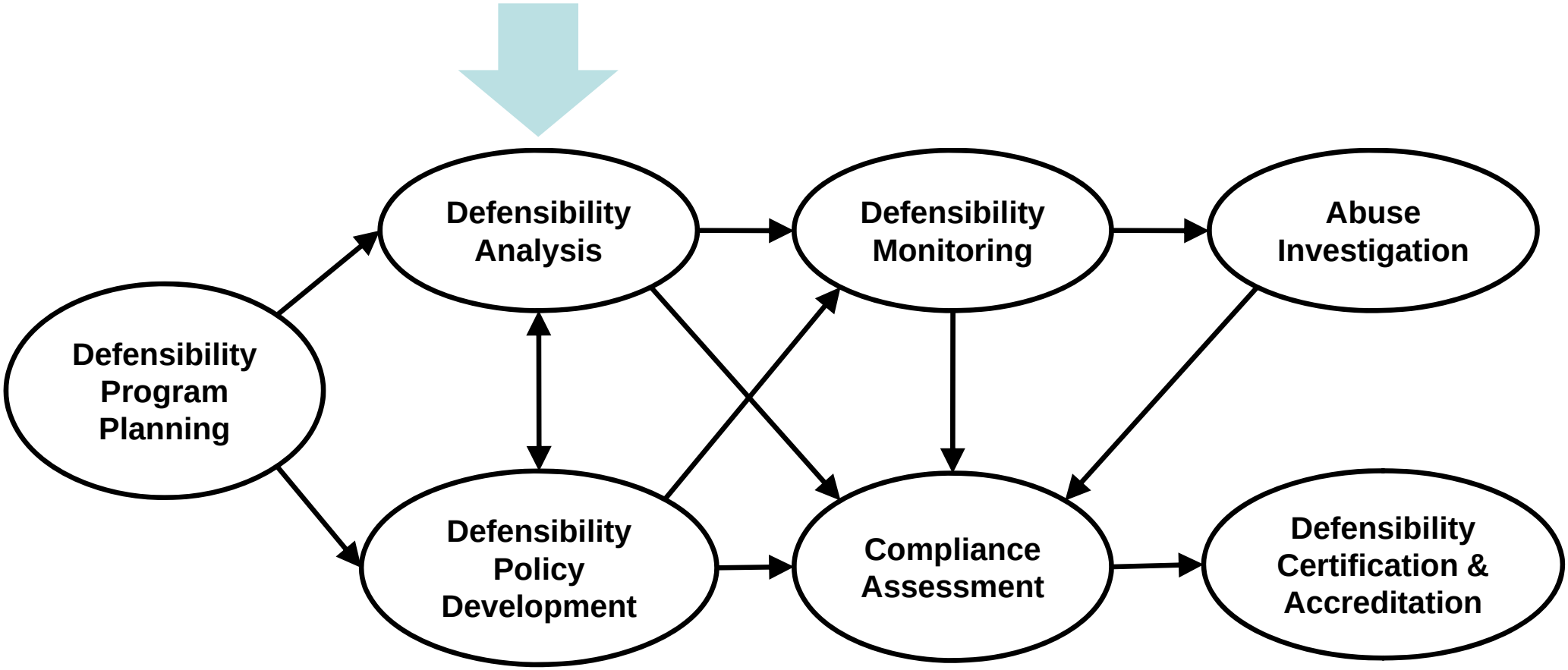
Better Integrate Safety and Security Methods with Requirements Methods:

- Early during Development Cycle
- Clearly define Team Responsibilities
- Provide Cross Training

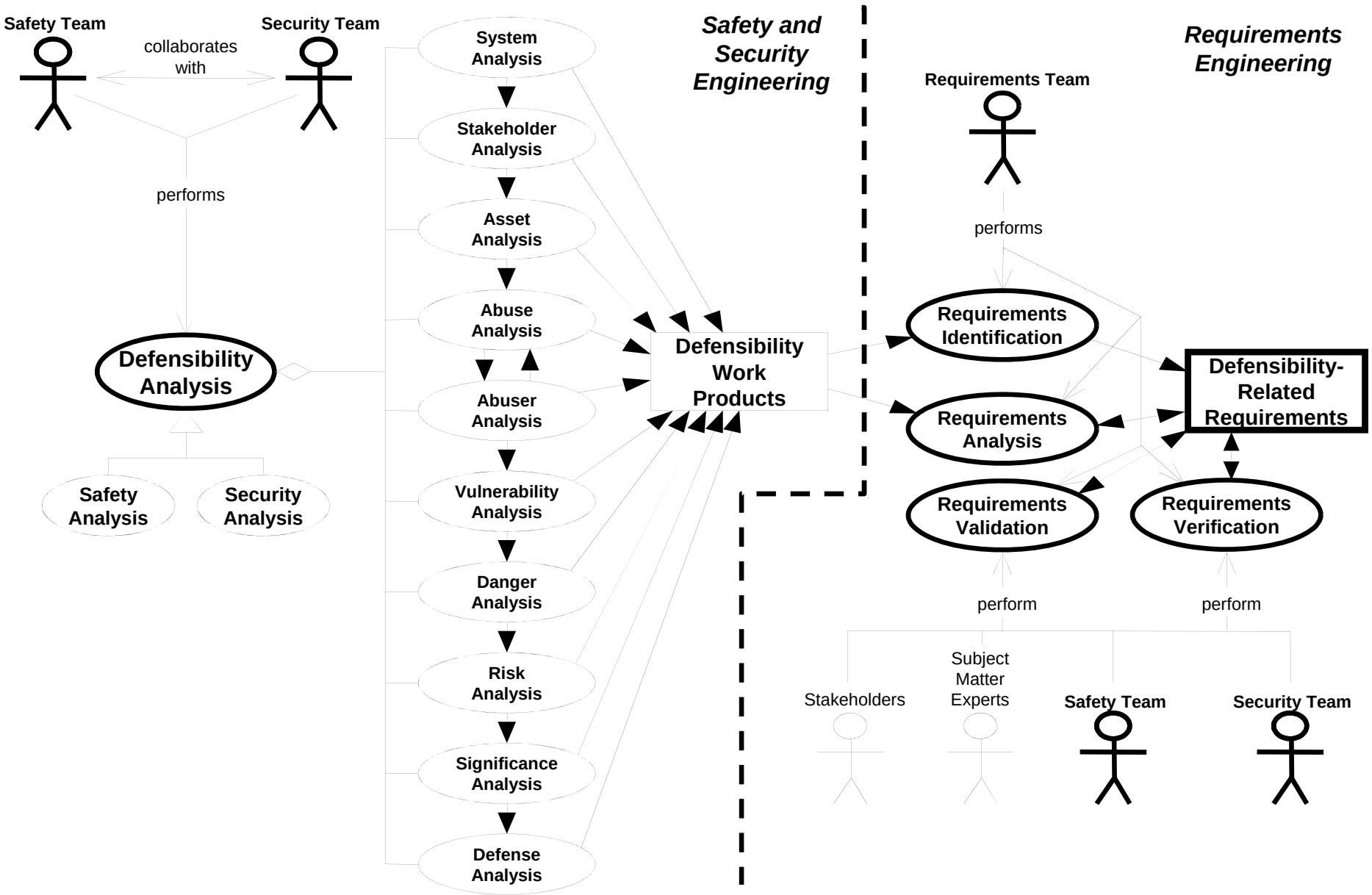
Develop all types of Safety- and Security-related Requirements

Ensure that these Requirements have appropriate Properties

An Overall Defensibility Engineering Method



Defensibility Analysis ➡ Reqts Engineering



Conclusion

Summary

Engineering safety- and security-related requirements requires appropriate Concepts / Methods / Techniques & Tools / Expertise

These must come from the respective experts in*:*

- Requirements engineering (safety- and security-related requirements)
- Safety engineering (analysis and safety goals)
- Security engineering (analysis and security goals)

BUT, Requirements/Safety/Security Engineering need to be:

- Properly interwoven.
- Consistent with each other.
- Performed collaboratively and in parallel (i.e., overlapping in time).

A collaborative process will advance Safety and Security Engineering to 1st class efforts

Ultimately, collaboration will improve the safety and security aspects of delivered systems

Contact Information

Donald Firesmith
Senior Member of the Tech. Staff
Acquisition Support Program
Telephone: +1 412-268-6874
Email: dgf@sei.cmu.edu

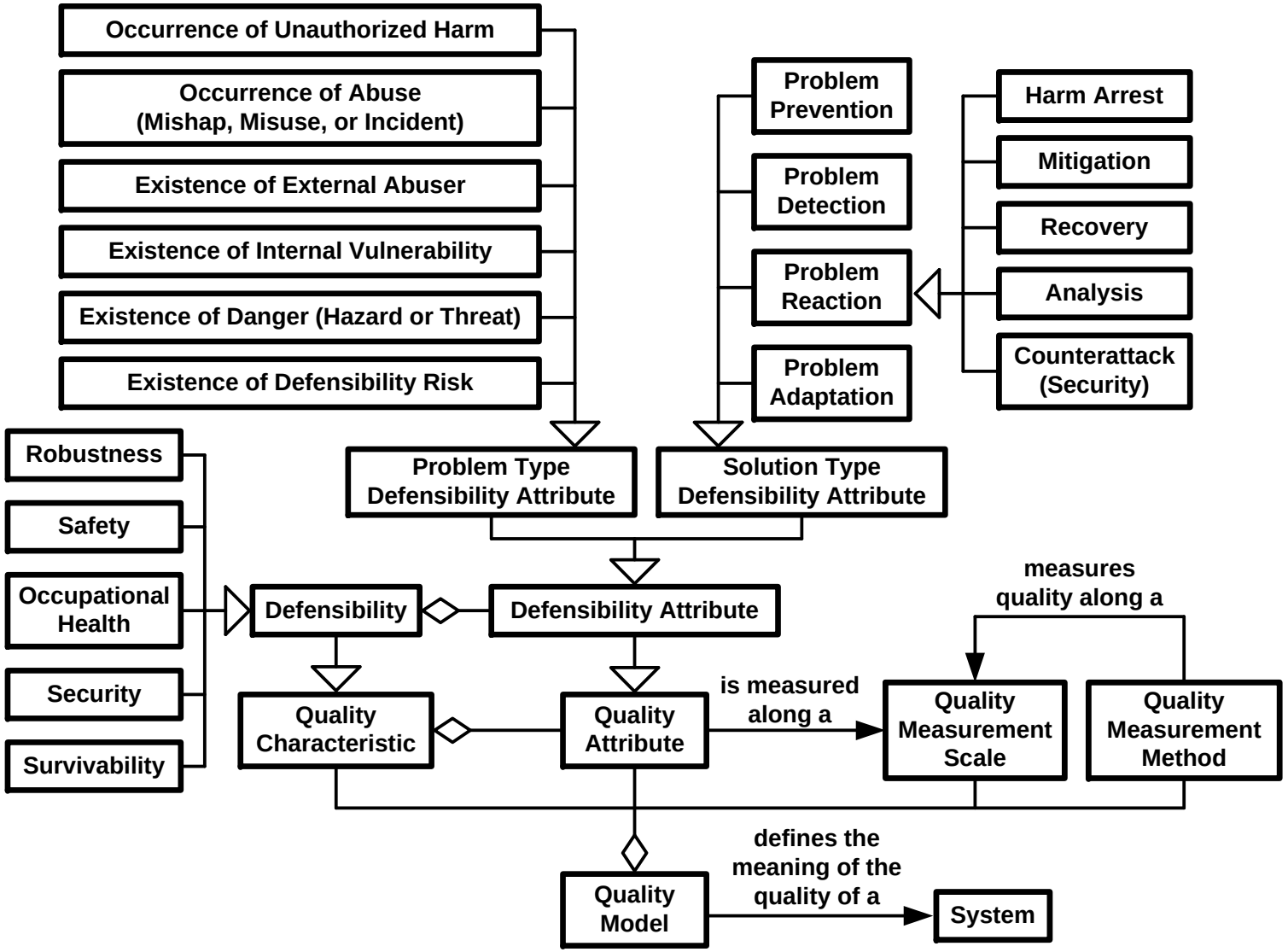
U.S. mail:
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

World Wide Web:
www.sei.cmu.edu
www.sei.cmu.edu/contact.html

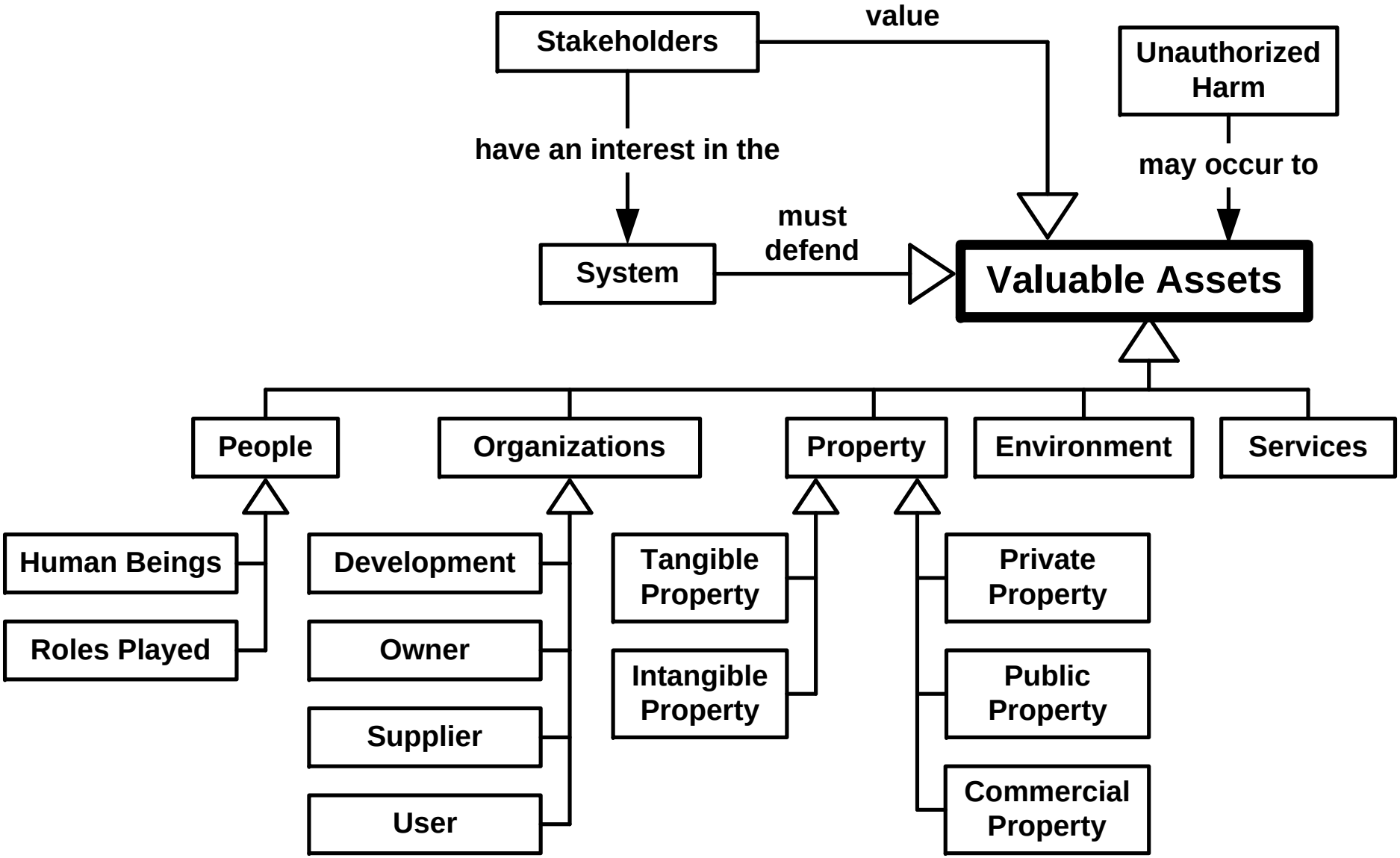
Customer Relations
Email: customer-relations@sei.cmu.edu
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257

Backup

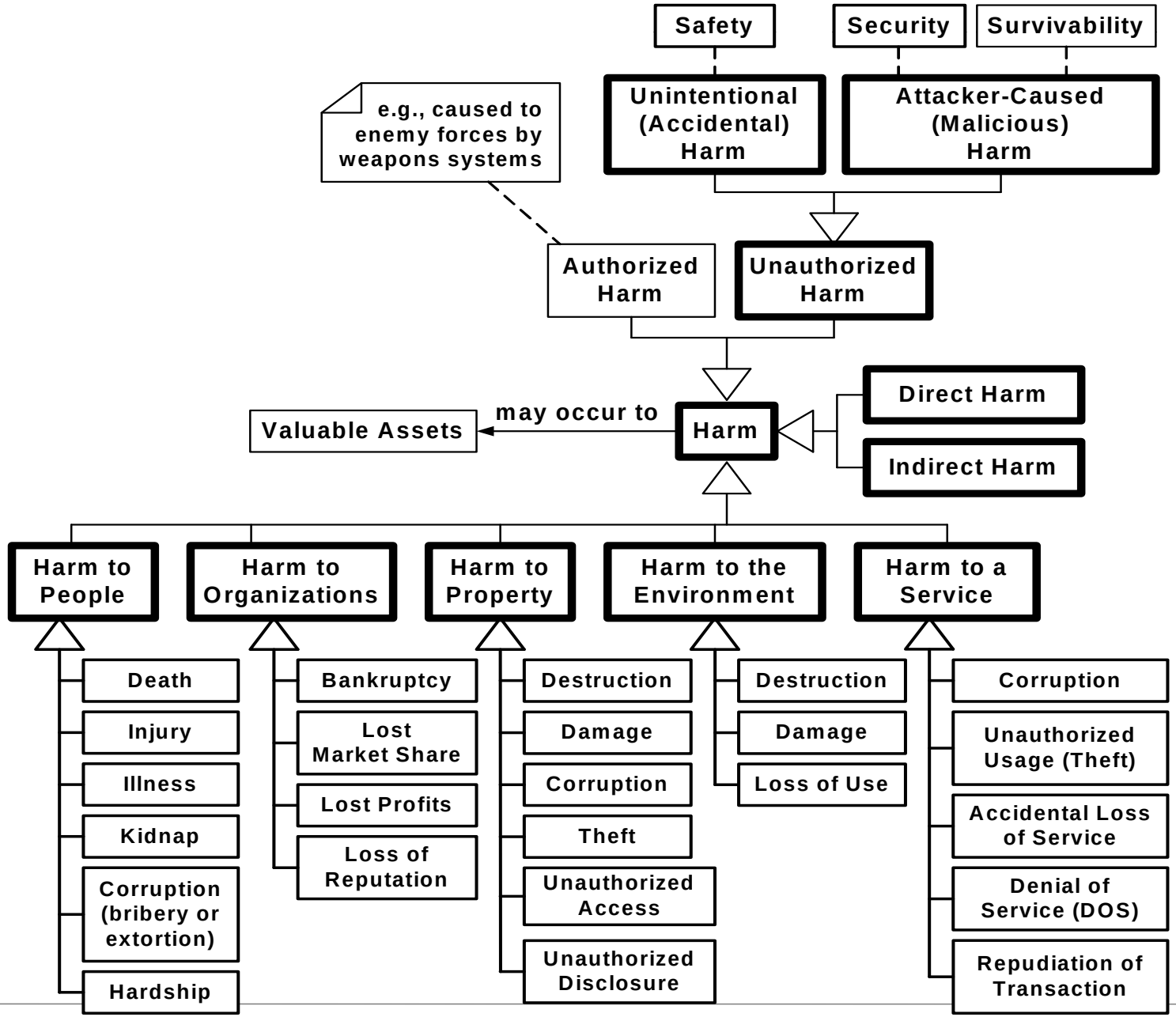
Defensibility Quality Attributes



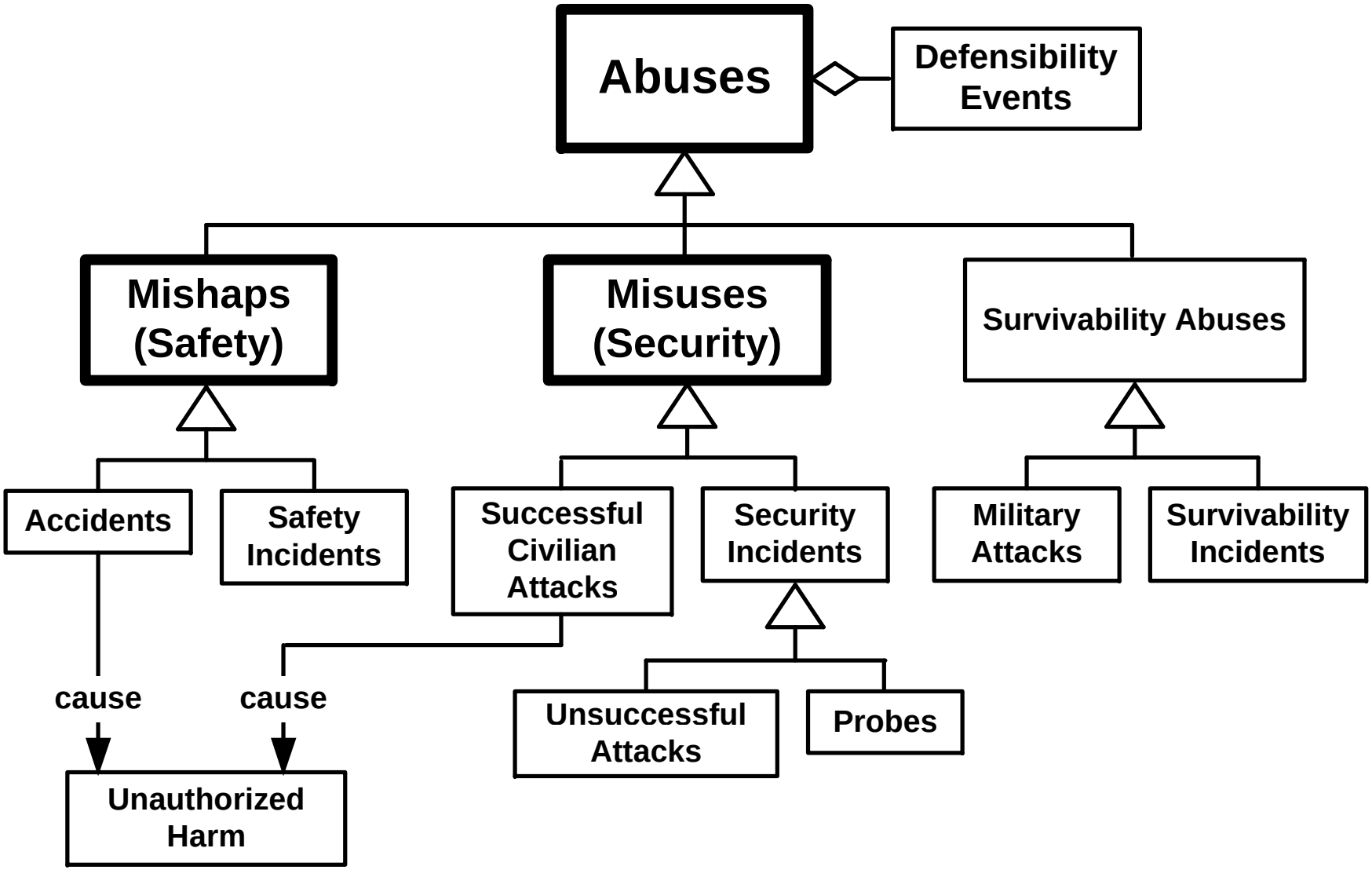
Unauthorized Harm to Valuable Assets



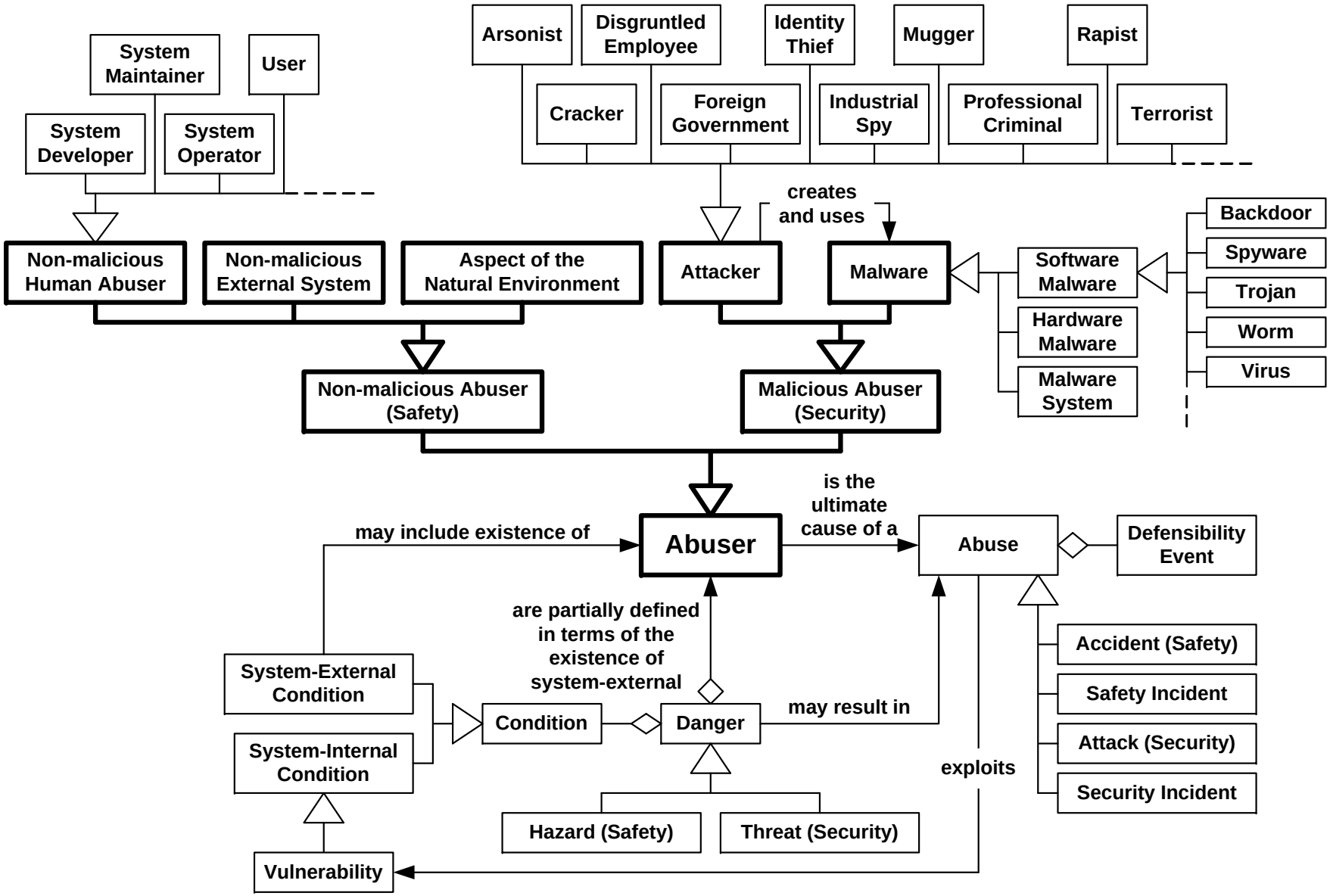
Types of Harm



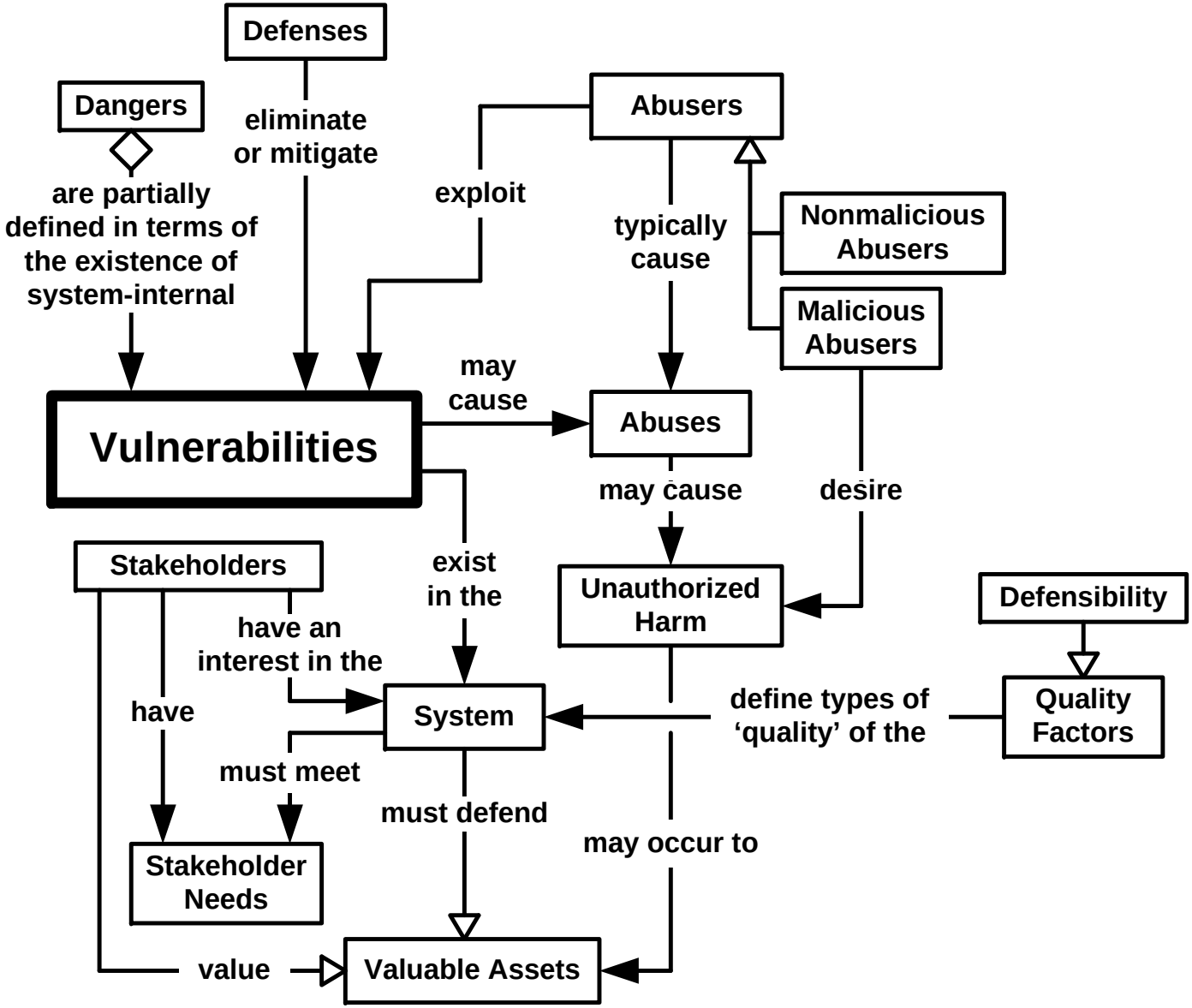
Types of Abuses



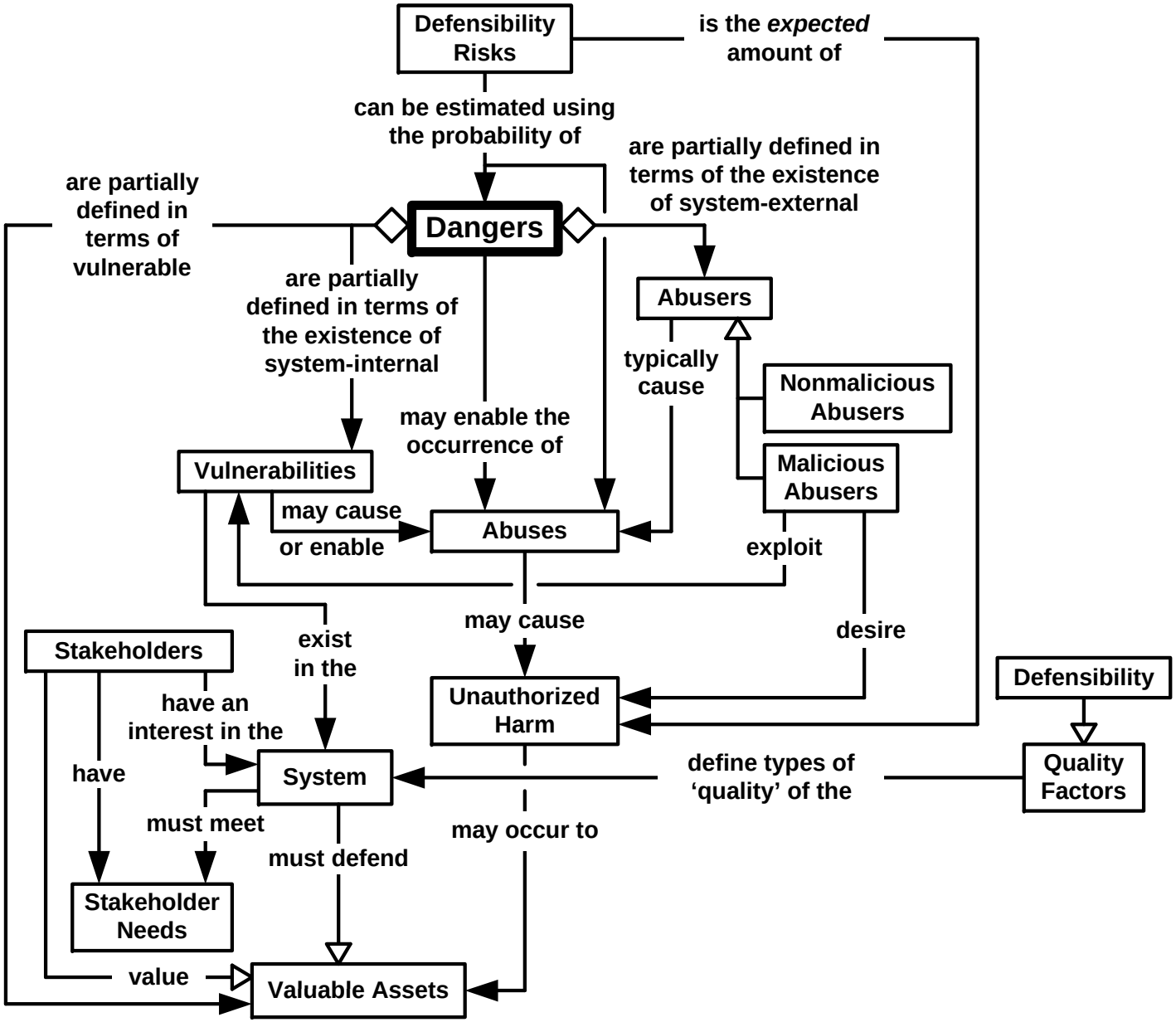
Types of Abusers



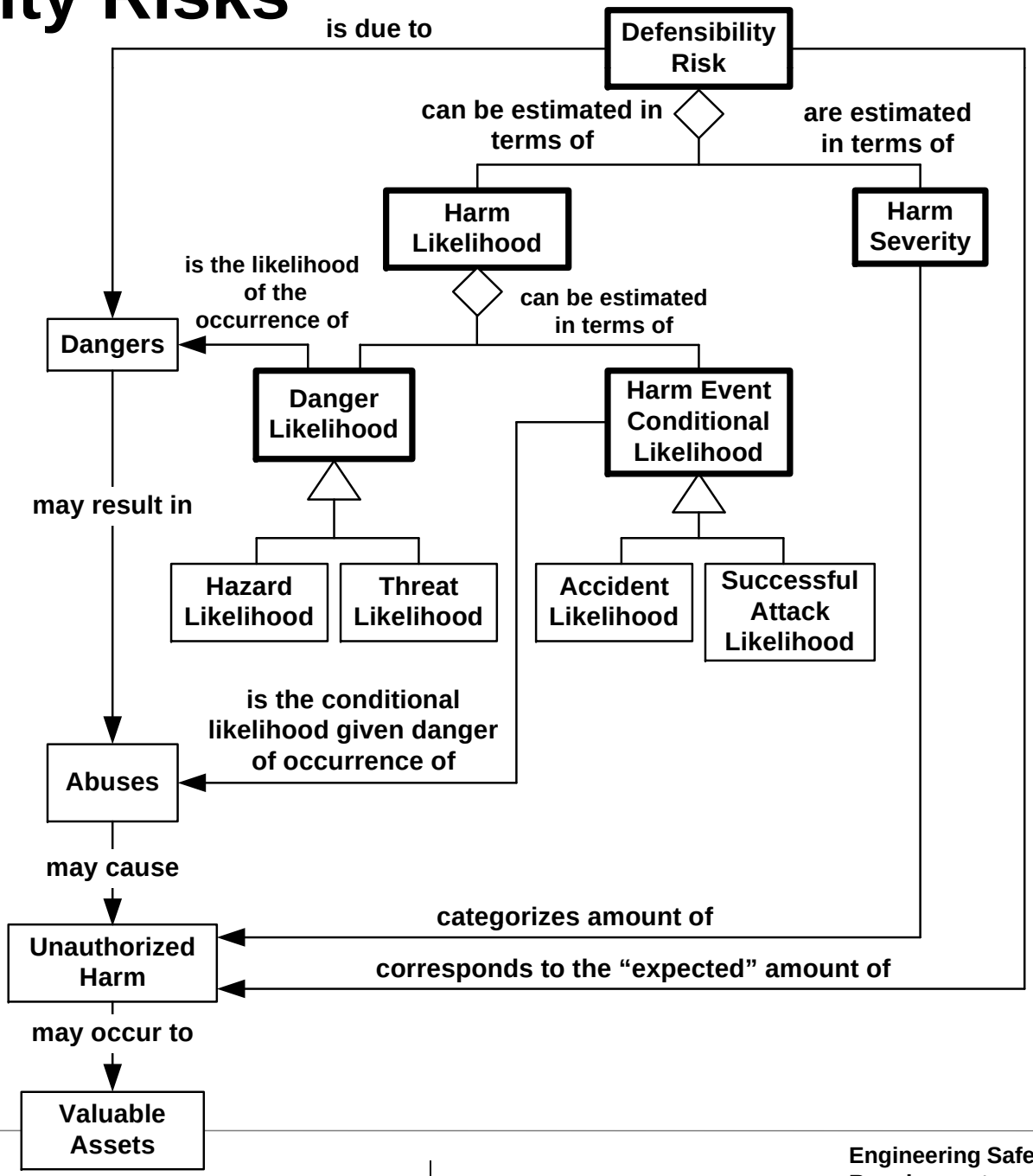
Vulnerabilities



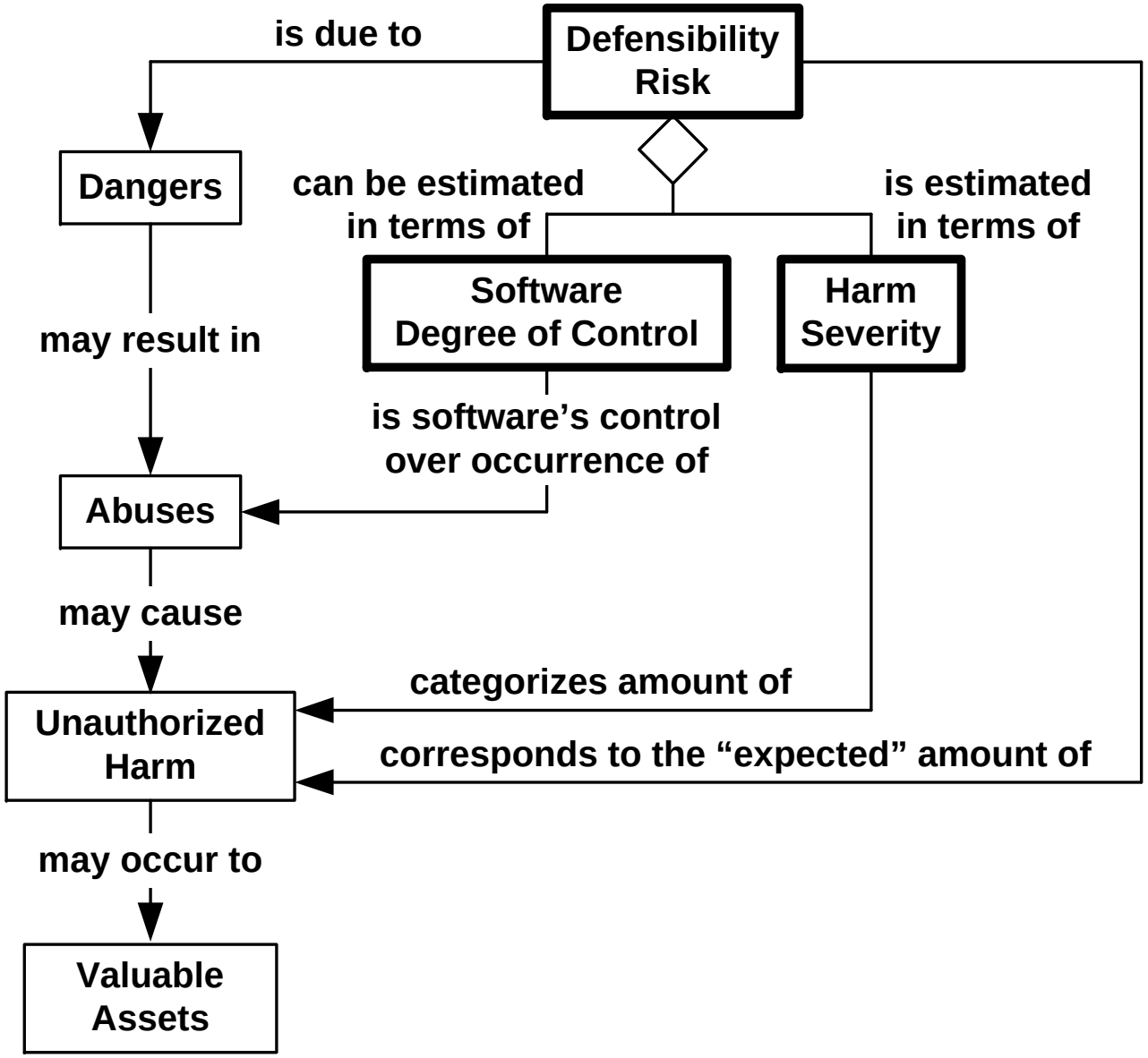
Dangers



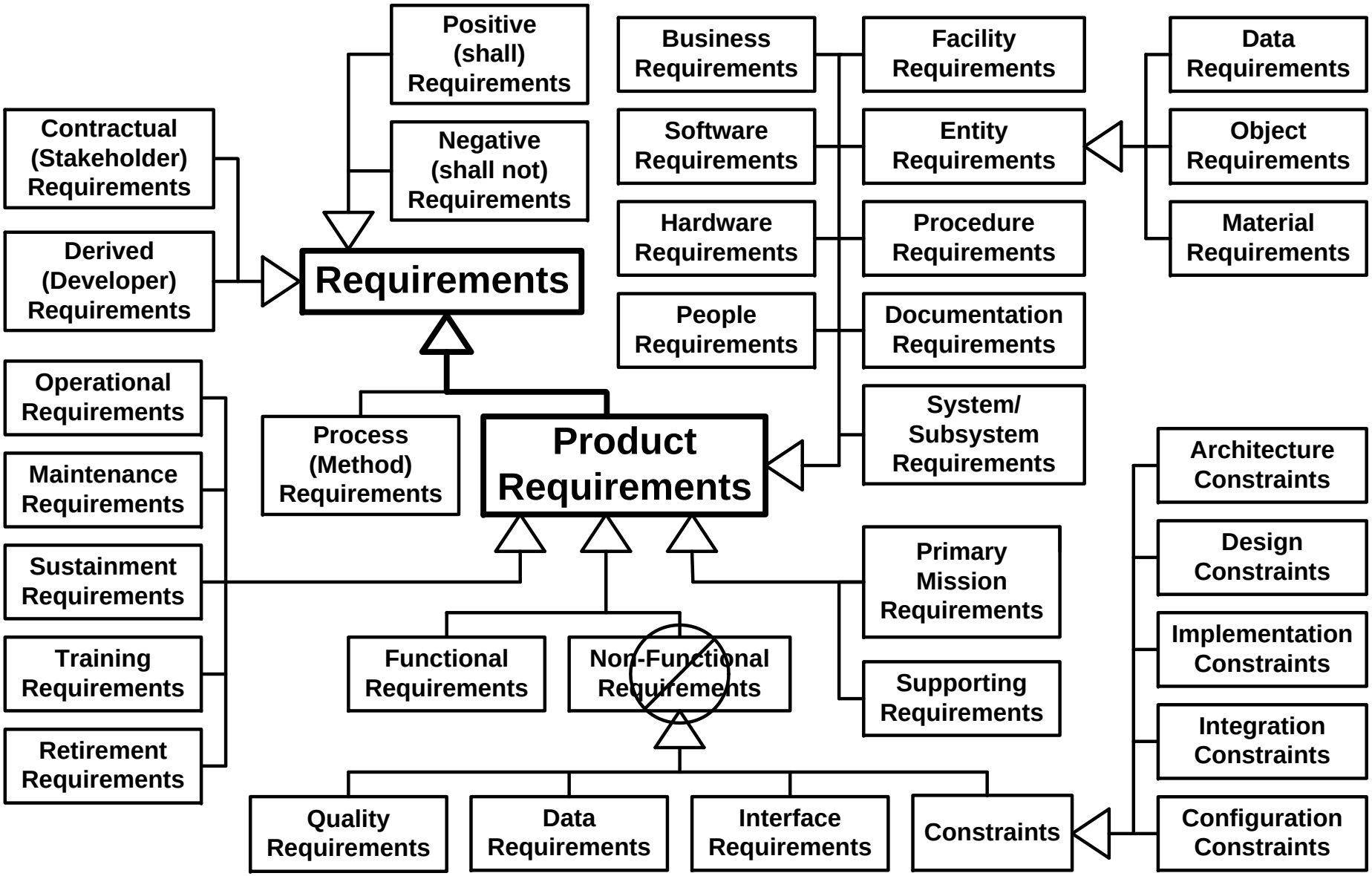
Defensibility Risks



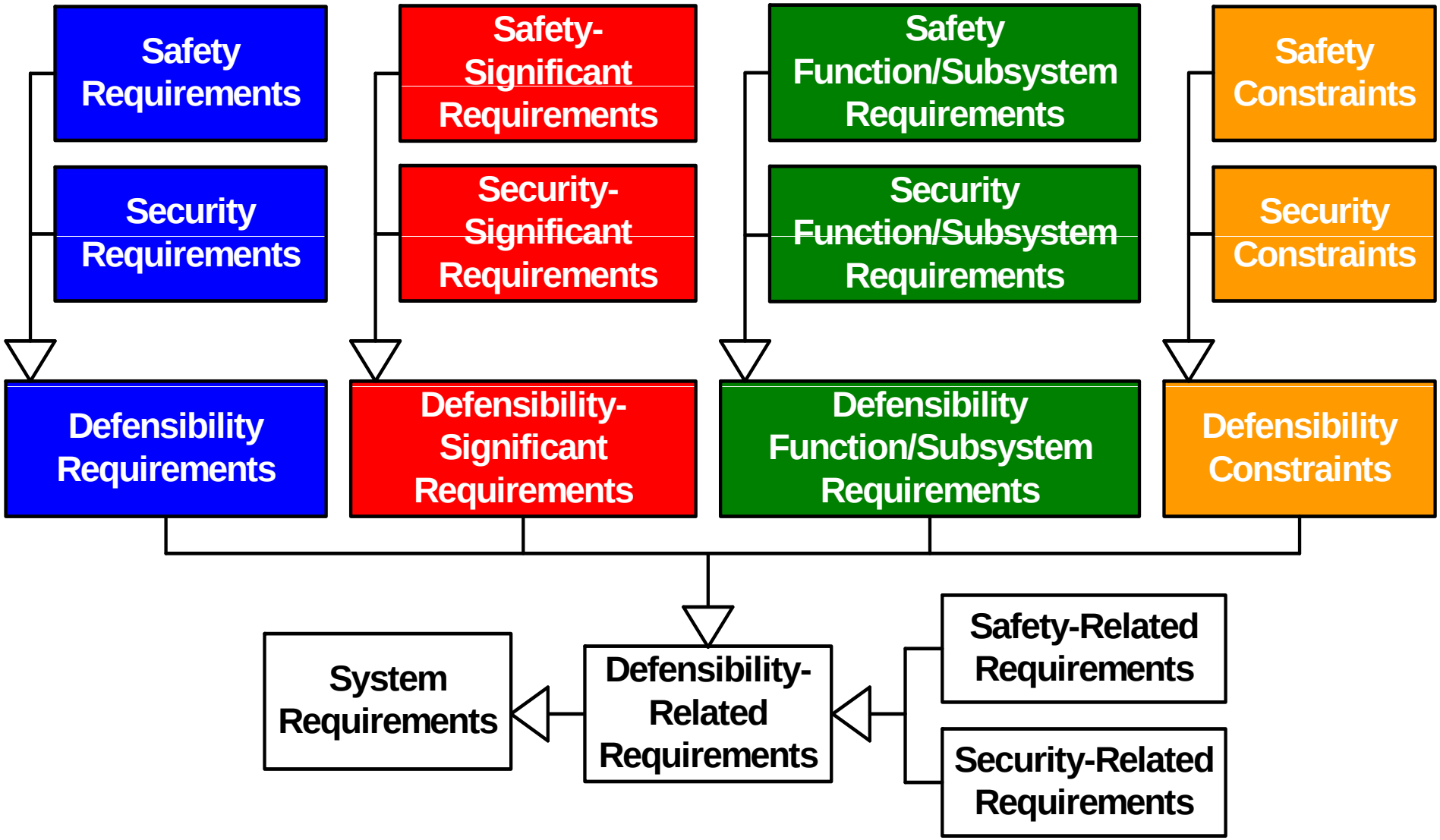
Risk in terms of Software Degree of Control



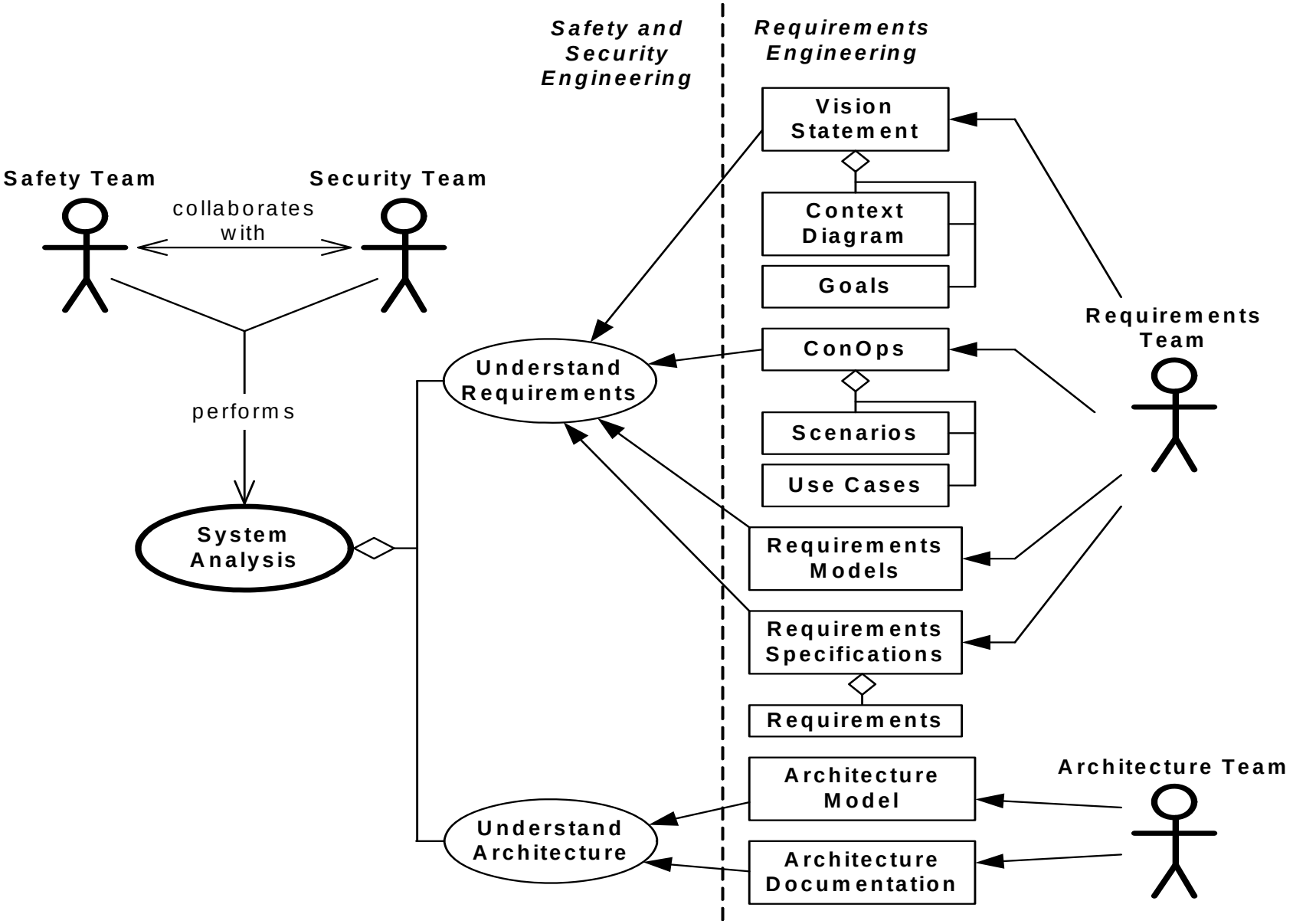
Types of Requirements



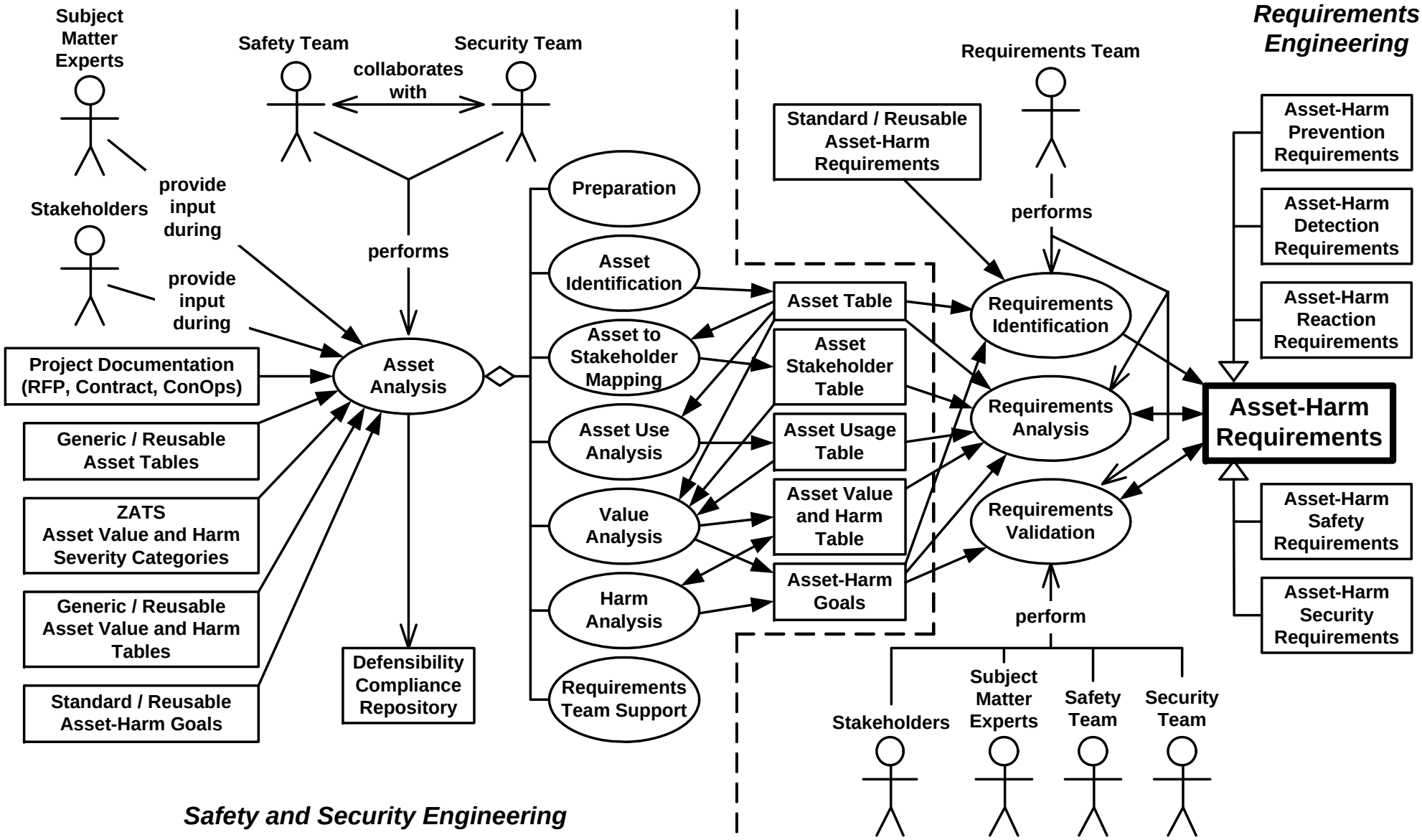
Types of Defensibility-Related Requirements



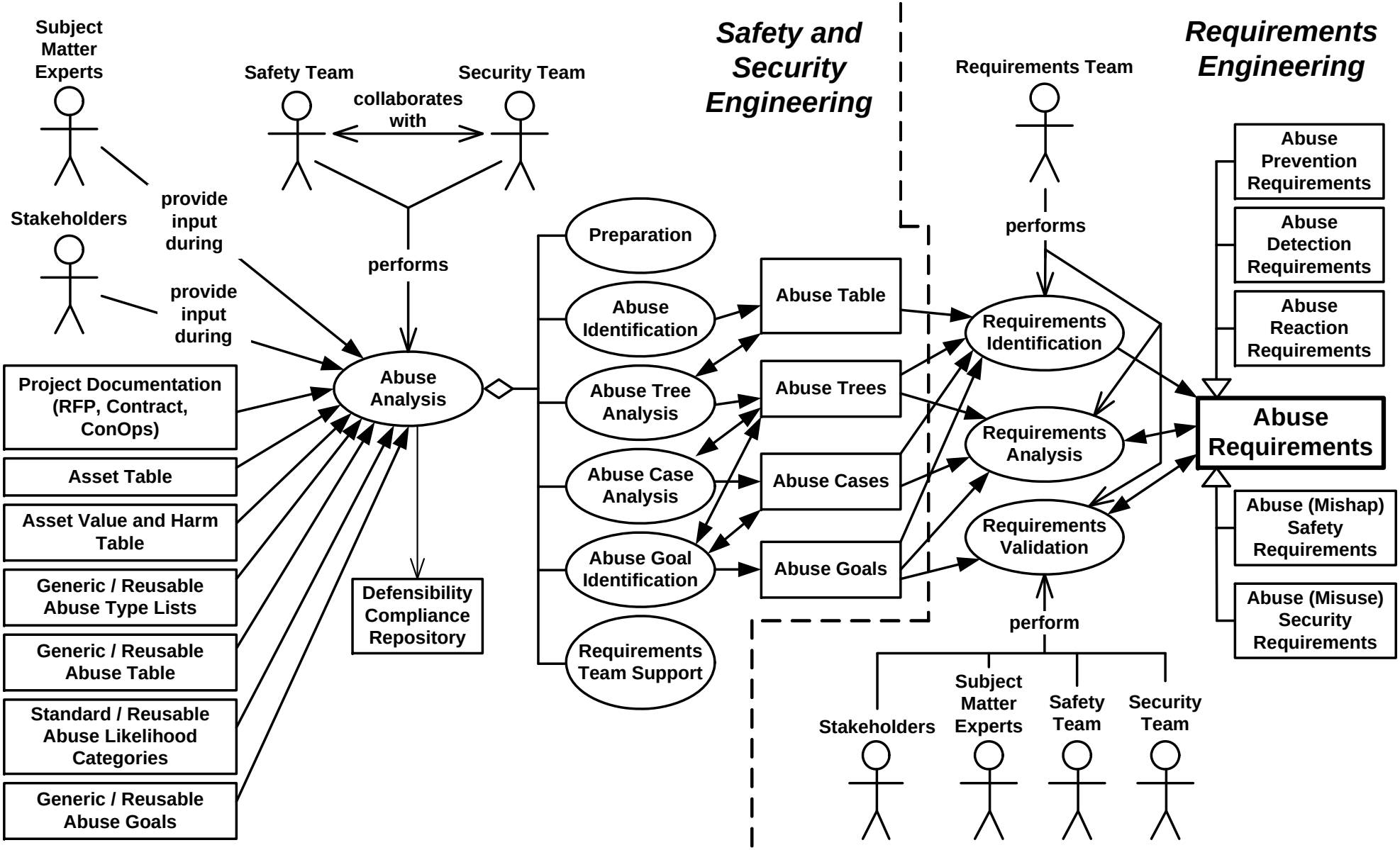
Systems Analysis



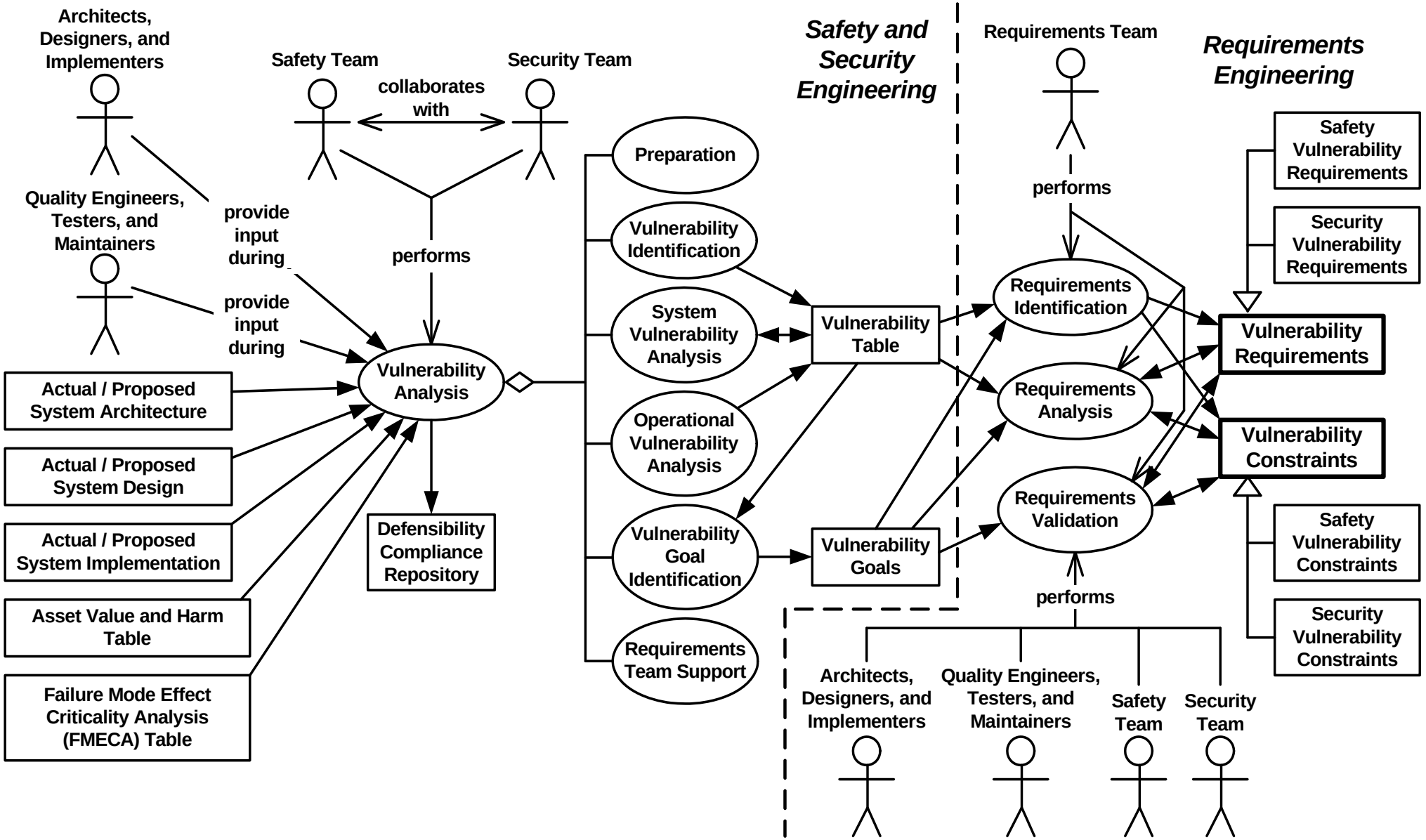
Asset Analysis



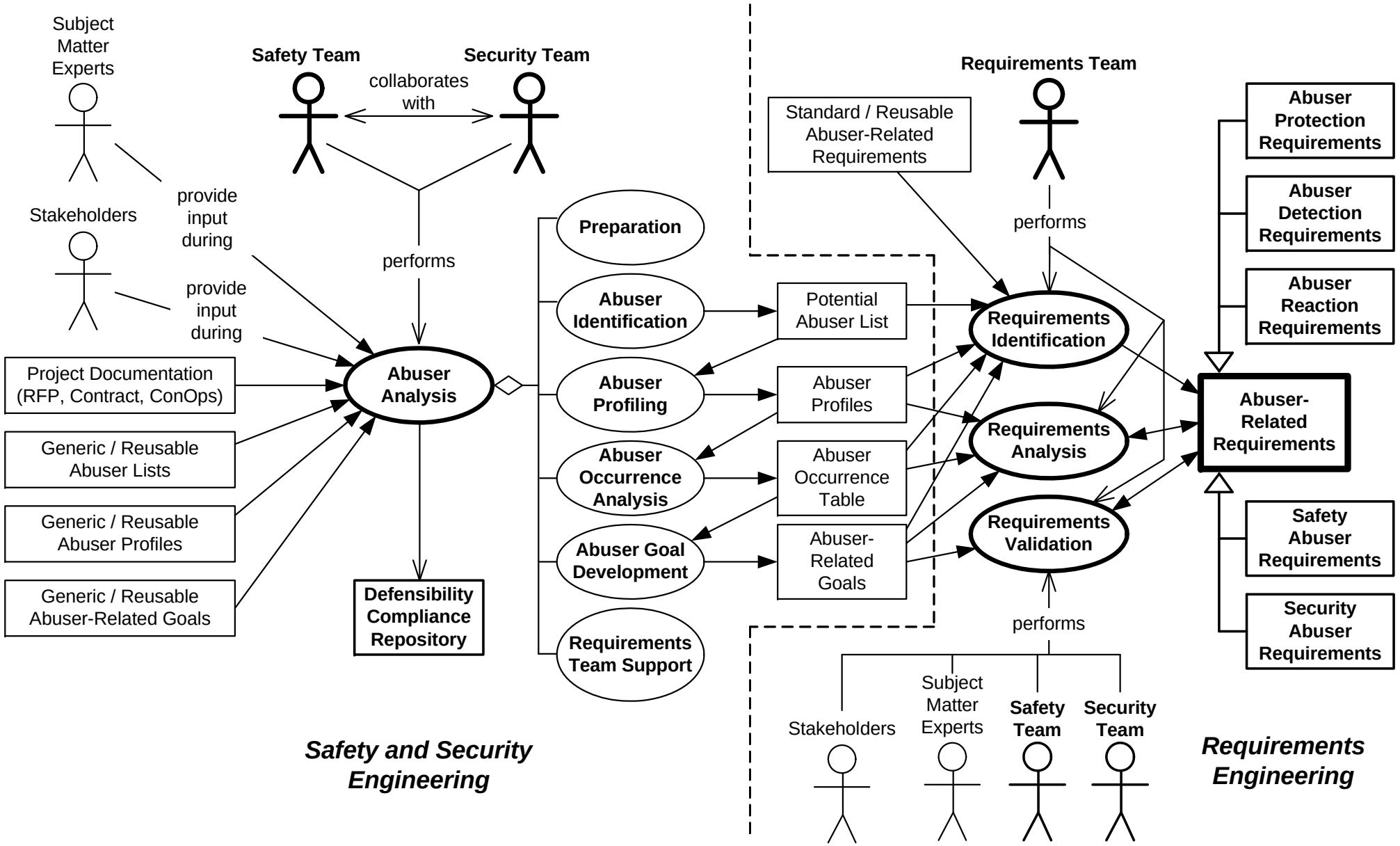
Abuse (Misuse and Mishap) Analysis



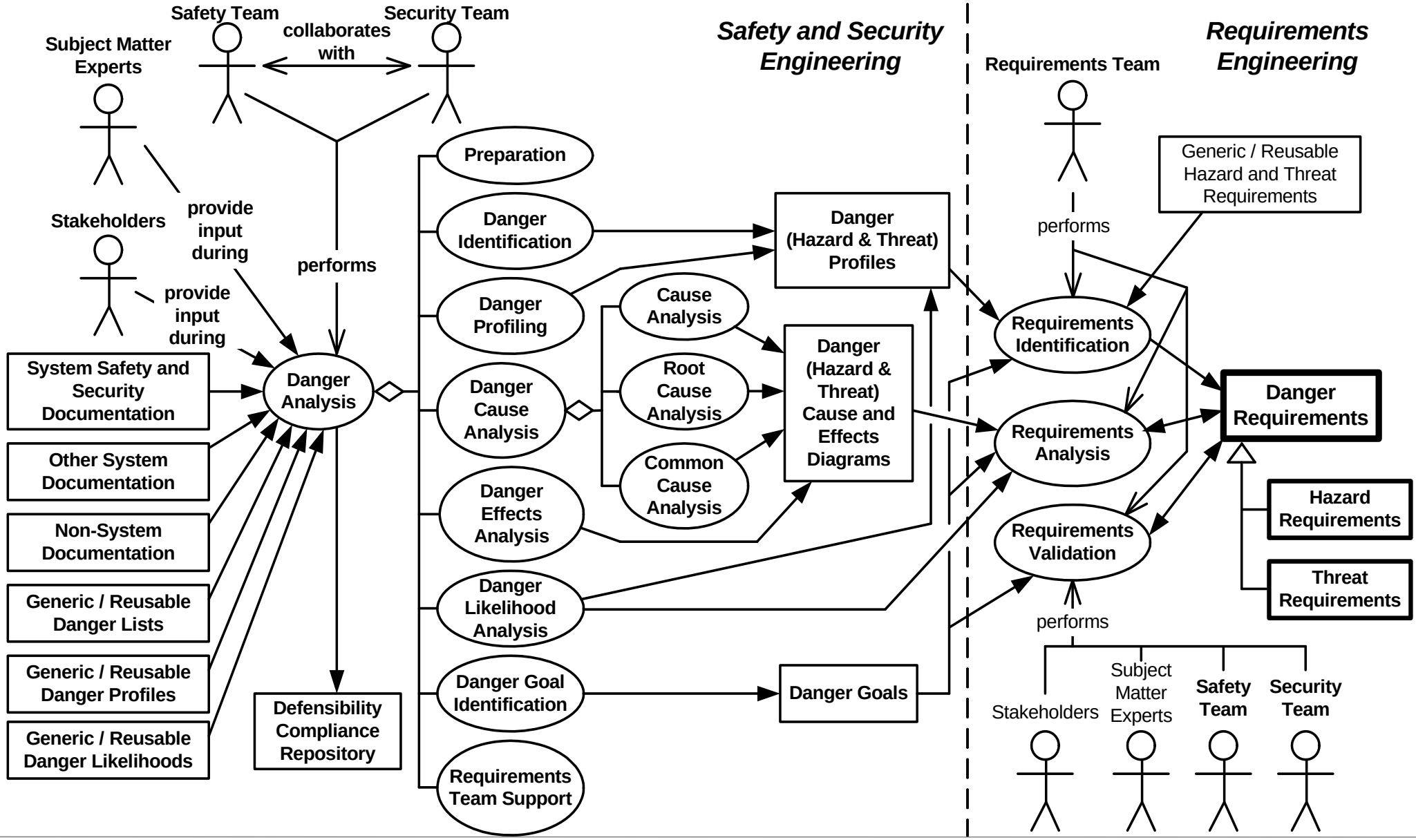
Vulnerability Analysis



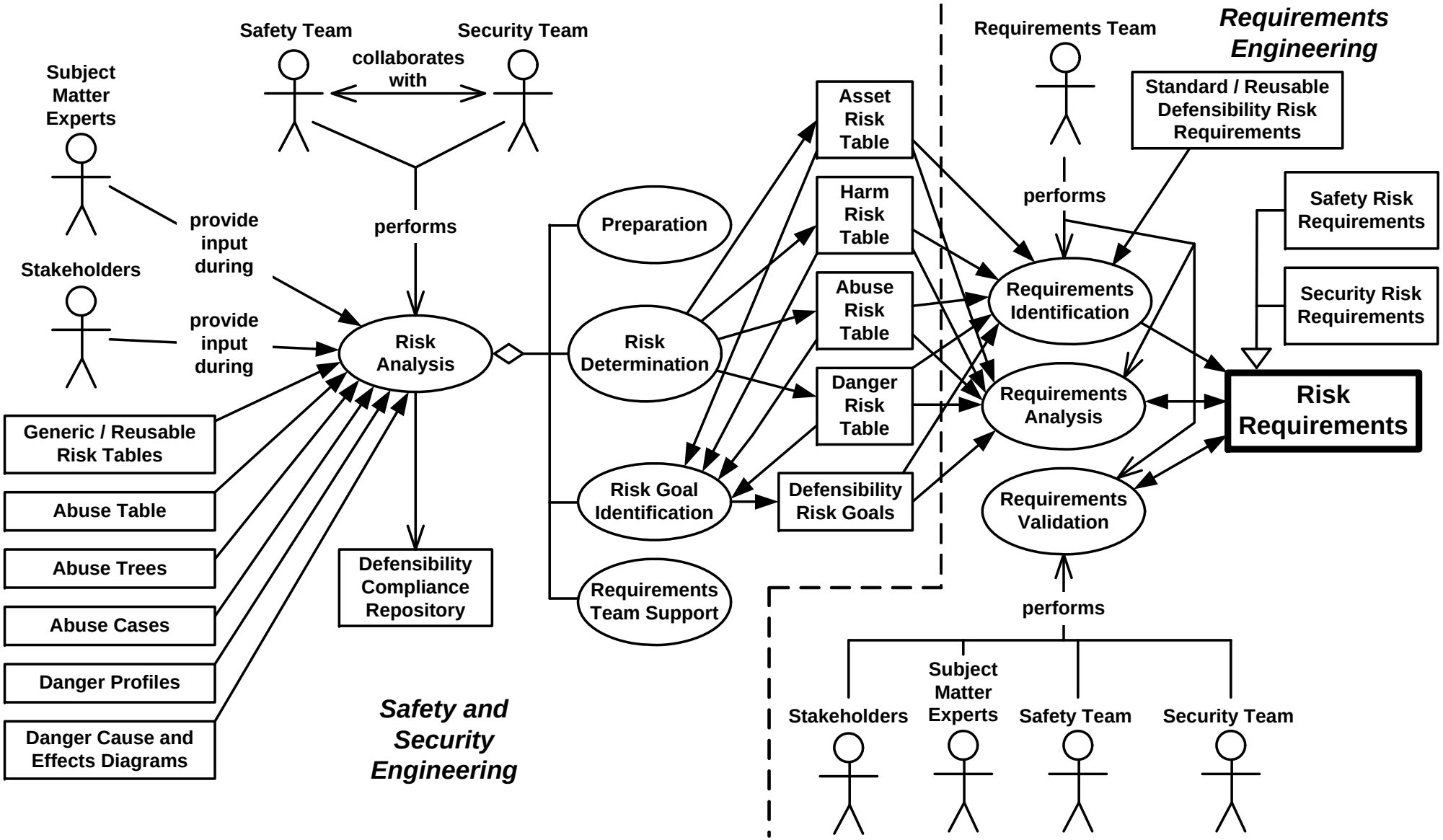
Abuser Analysis



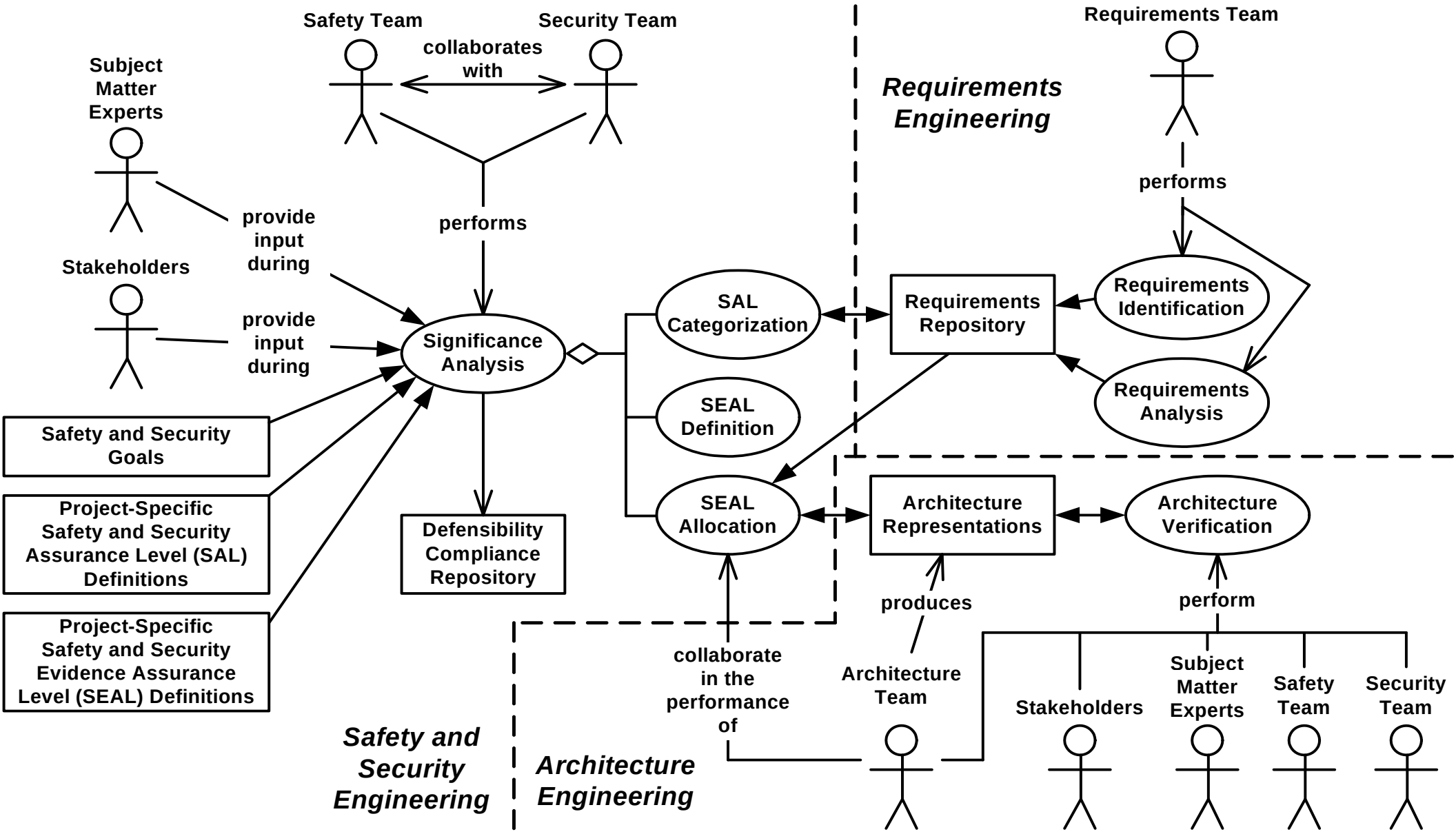
Danger Analysis



Defensibility Risk Analysis



Defensibility Significance Analysis



Defense Analysis